

REMARKS

In the Office Action, the Examiner rejected Claims 1-20, which were all of the then pending claims, under 35 U.S.C. 103 as being unpatentable over a document titled "P-Synch Installation and Administration Guide," (P-Synch) Document Revision 4,50, and dated June 1, 2000, in view of a printed web page titled "Using Privacy Features" (Mozilla). The Examiner also objected to Claims 3, 8 and 14 as being substantial duplicated of other claims, and objective to an informality in Claim 20.

It is noted that the previous rejection of the claims under 35 U.S.C. 102 based upon an alleged public use or sale of the invention, was withdrawn.

Independent Claims 1, 7 and 13 are being amended to better define the subject matters of these claims, and Claim 20 is being amended to address the informality noted by the Examiner and to elaborate on features of an embodiment of the invention. Also, Claims 3, 8 and 14 are being cancelled.

In view of the cancellation of Claims 3, 8 and 14, it is believed unnecessary to discuss these claims further herein.

With respect to Claim 20, the Examiner, in the Office Action, noted that the phrase "user profile tables" was recited twice in one list, and this opportunity is being taken to one occurrence of this phrase in this list. The Examiner is, hence, respectfully asked to reconsider and to withdraw the objection to Claim 20.

Moreover, Claims 1, 2, 4-7, 9-13 and 15-20, which are now all of the pending claims, patentably distinguish over the prior art and are allowable because the prior art does not disclose or render obvious the comprehensive password change tool or method described in independent Claims 1, 7 and 13. In particular, the prior art does not disclose or render obvious storing the

complete set of information described in Claims 1, 7 and 13, and using a script to simulate key stroke entries to perform a password change, as now required by Claims 1, 7 and 13.

For example, the "P-Synch" document describes a password management application, referred to as "P-Synch." With this application, a user specifies the password to change to, or to reset, and P-Synch runs through its list of targets in the background. An administrator defines which machines and applications a user can modify passwords on, as well as more advanced options such as password aging.

As described in the article, "P-Synch" uses either a native API or TELNET to log in to each machine or application one at a time, and runs whatever commands are necessary to modify the passwords. The user only needs to specify the password to change to (or to reset) and P-Synch, as mentioned above, runs through its list of targets in the background.

With the present invention, the password change tool has much more information, and also operates in a different way. In the implementation of the present invention, the user begins the process by invoking a tool or a password management facility. That tool or facility then displays a list of the passwords, a description of the computer applications for which those passwords are used, a description of a procedure for changing the password, and a graphical user interface that is then invoked to change the password. Also, this tool stores a considerable amount of information including, for each application the tool is used with, a description of the application, a description of the password type for the application, current and previous passwords for the application, a Uniform Resource Locator for the application, executable code and parameters needed to change the password for the application, and readable instructions for changing the password.

This process is of significant utility because it provides a very simple and complete

process to manage changing multiple passwords, and that can be used to ensure multiple levels of security.

More specifically, the present invention provides an application that allows a person to define in a secure way a multitude of passwords as well as what actions they need to take to initiate a password change. In accordance with one embodiment of the invention, the above-mentioned tool is provided for maintaining passwords. This tool comprises storage for a plurality of current passwords for a plurality of respective applications, and means for displaying a reminder to change one or more of those passwords.

A script is provided for simulating keystroke entries to automatically perform a password change in said respective applications for said current passwords of said reminder. In addition, the tool storage also holds considerable information about the applications. For example, this storage, as mentioned above, holds, for each of the group of applications, a description of the application, a description of the password type, the current and the previous passwords for the application, and a uniform resource locator for the application. The tool also holds executable code and parameters needed to change the password for the application, and readable instructions for changing the password.

When the tool is invoked, it displays a list of the passwords, a description of the computer applications for which those passwords are used, a description of a procedure for changing the password, and a graphical user interface. This graphical user interface is then used to invoke the scripts that, in turn, are used to change the passwords.

As the Examiner has recognized, there are a number of important differences between the present invention and the manager and method disclosed in the cited P-synch document. One very important difference is that with the present invention, both current and past passwords are

stored in the tool.

In order to address the deficiency of the P-Synch document, the Examiner relies on Mozilla for its disclosure of a password manager tool with storage for a user's current passwords. With the present invention, however, the tool stores both current and previous passwords.

This combination – that is, storing both previous and current passwords – is useful because it may be used to better monitor the use of passwords. The tool of the present invention, when determining if a proposed password is acceptable, can compare that password, not only to the current password and to various rules, but also to previous passwords. The tool may look for patterns that might be security risks.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or render obvious the above-discussed aspect of the present invention.

Independent Claims 1, 7 and 13 are being amended to better emphasize the above-discussed aspects of the present invention. In particular, Claim 1, which is directed to a tool for maintaining passwords, is being amended to set forth positively the limitation that the tool stores, for each of a group of applications, a description of the application, a description of the password type for the application, current and previous passwords for the application, a Uniform Resource Locator for the application, executable code and parameters needed to change the password for the application, and readable instructions for changing the password. Claim 1, as presented herewith, also includes the limitation that the script that is invoked to change the passwords does so by simulating keystroke entries.

Claim 7 is drawn to a method for managing passwords to computer applications, and Claim 13 is directed to a program storage device. Both of these claims, analogous to Claim 1,

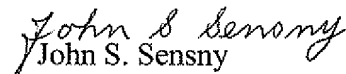
include the limitation of storing in the password management facility, for each of a group of applications, a description of the application, a description of the password type for the application, current and previous passwords for the application, a Uniform Resource Locator for the application, executable code and parameters needed to change the password for the application, and readable instructions for changing the password. These Claim 7 and 13, as presented herewith, also includes the limitation that the script that is invoked to change the passwords does so by simulating keystroke entries.

In light of the above-discussed differences between Claims 1, 7 and 13 and the prior art, and because of the advantages associated with those differences, Claims 1, 7 and 13 patentably distinguish over the prior art and are allowable. Claims 2, 4-6 and 19 are dependent from, and are allowable with, Claim 1. Also, Claims 9-12 and 20 are dependent from Claim 7 and are allowable therewith; and Claims 15-18 are dependent from, and are allowable with, Claim 13.

For the reasons discussed above, the Examiner is respectfully requested to reconsider and to withdraw the rejection of Claims 1, 2, 4-7, 9-13 and 15-20 under 35 U.S.C. 103, and to allow these claims.

If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this application, the Examiner is asked to telephone the undersigned.

Respectfully submitted,


John S. Sensny
Registration No. 28,757

SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 Garden City Plaza, Suite 300
Garden City, New York 11530
516-742-4343
JSS/ech